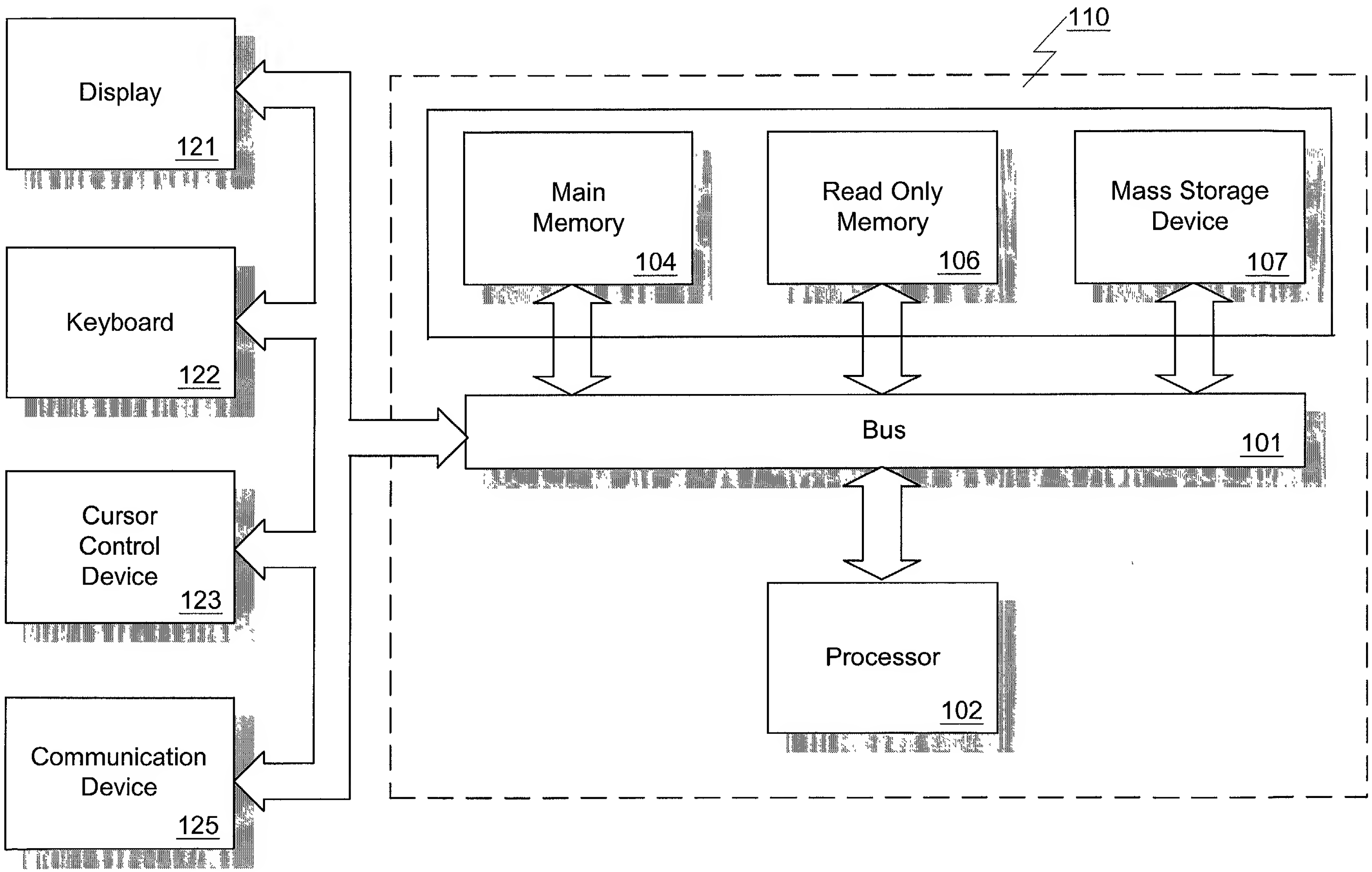
110
Display
121
Keyboard
122
Cursor
Control
Device
123
Communication
Device
125
Main
Memory
104
Read Only
Memory
106
Mass Storage
Device
107
Bus
101
Processor
102
100

Figure 1

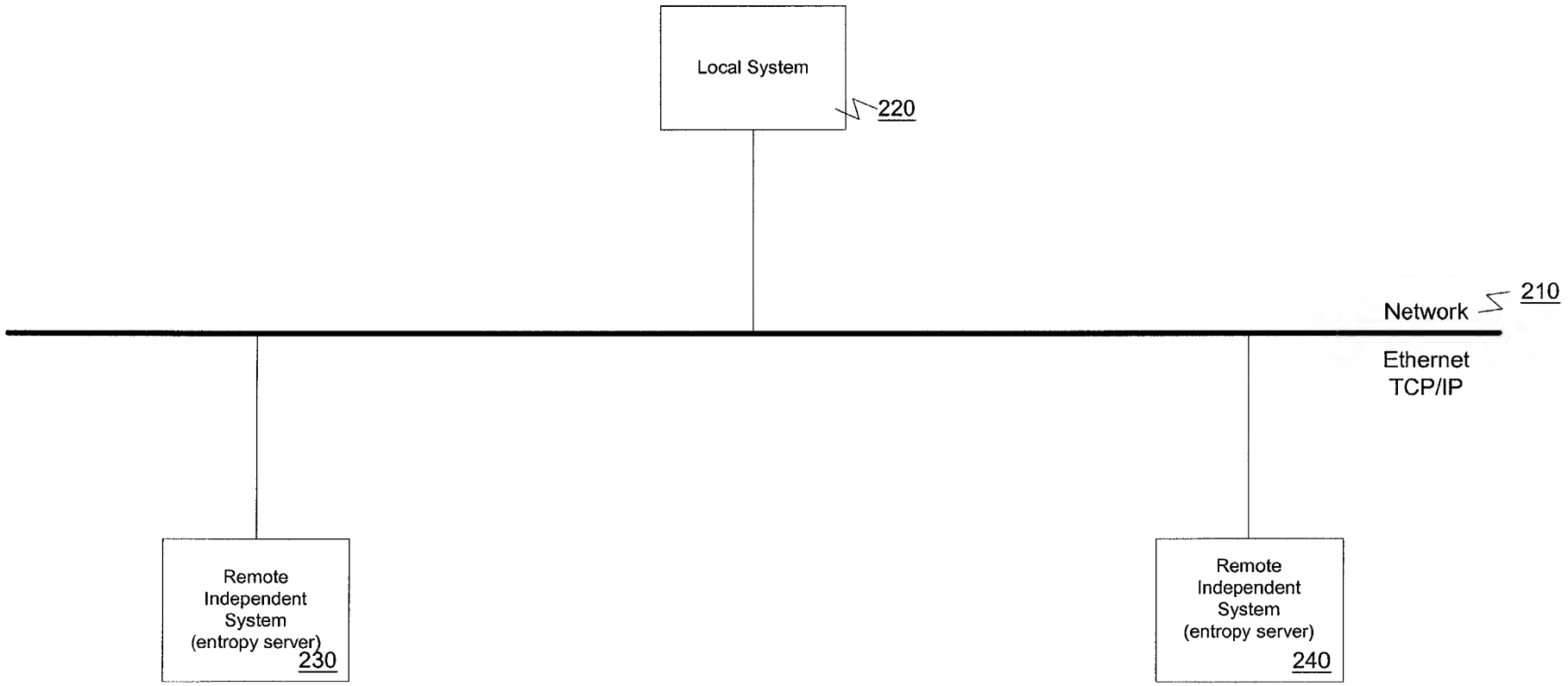

Figure 2

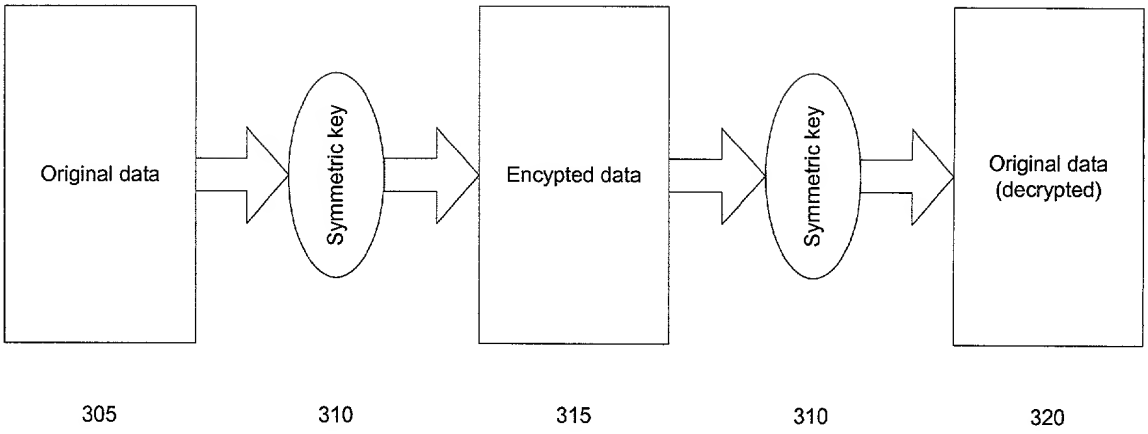

Figure 3A

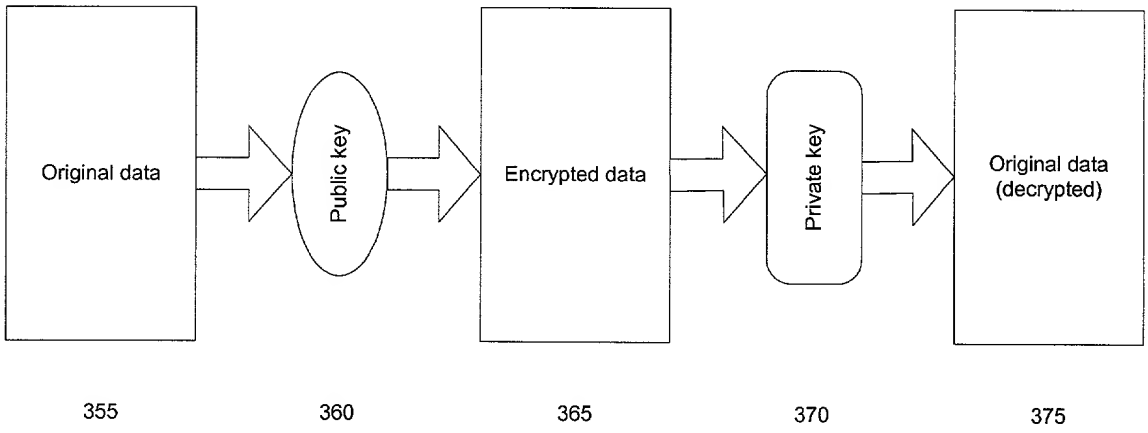

Figure 3B

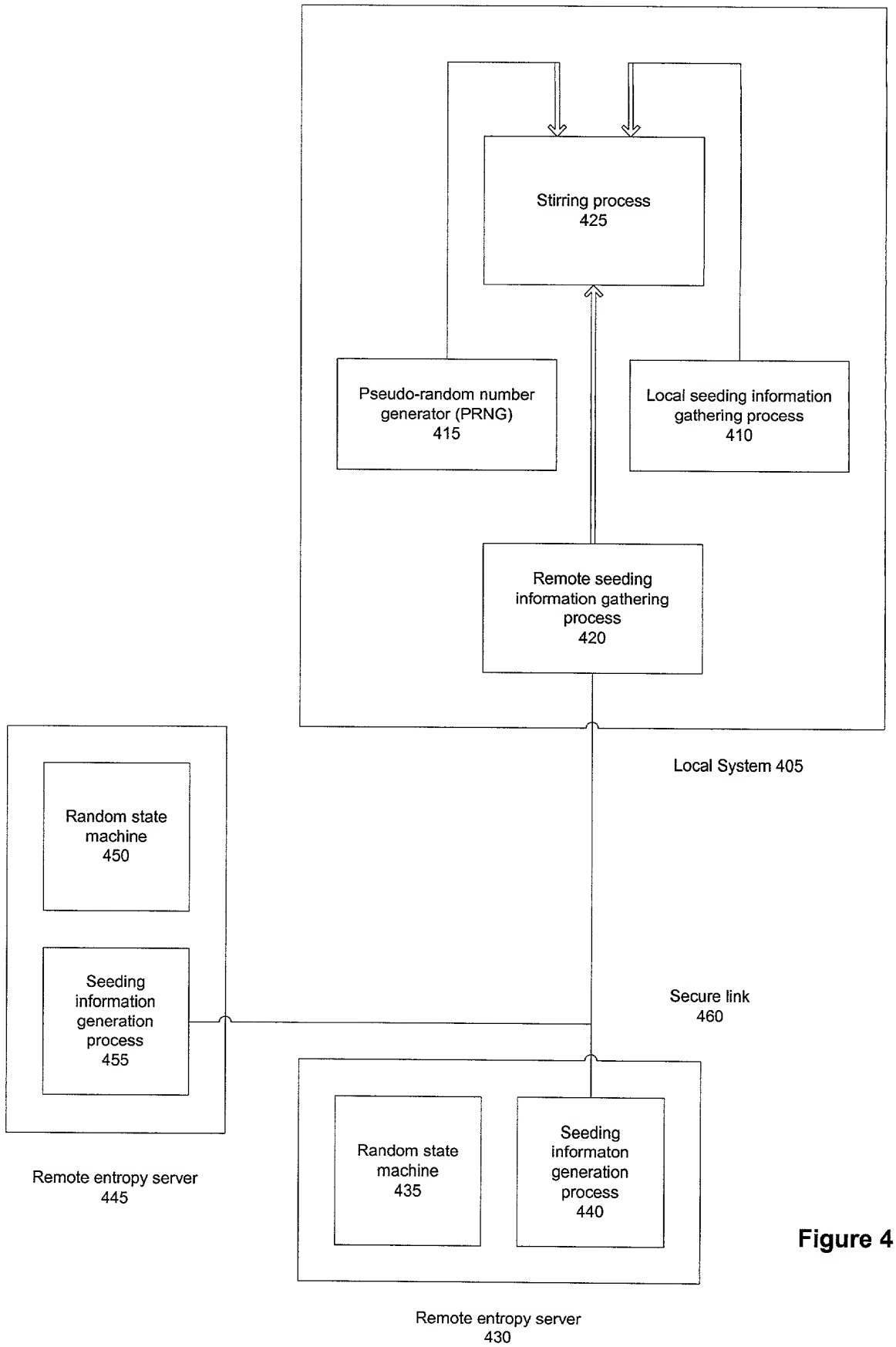
Stirring process
425
Pseudo-random number generator (PRNG)
415
Local seeding information gathering process
410
Remote seeding information gathering process
420
Local System 405
Random state machine
450
Seeding information generation process
455
Secure link
460
Random state machine
435
Seeding informaton generation process
440
Remote entropy server
445
Remote entropy server
430

Figure 4

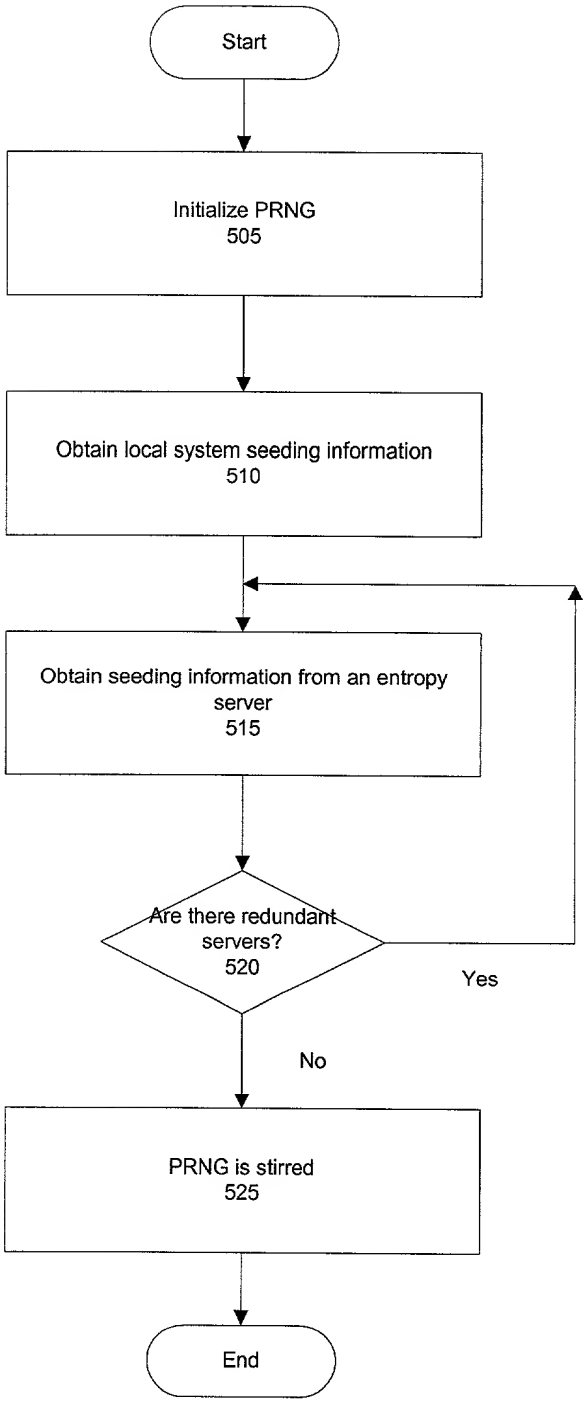
Start
Initialize PRNG
505
Obtain local system seeding information
510
Obtain seeding information from an entropy server
515
Are there redundant servers?
520
Yes
No
PRNG is stirred
525
End

Figure 5

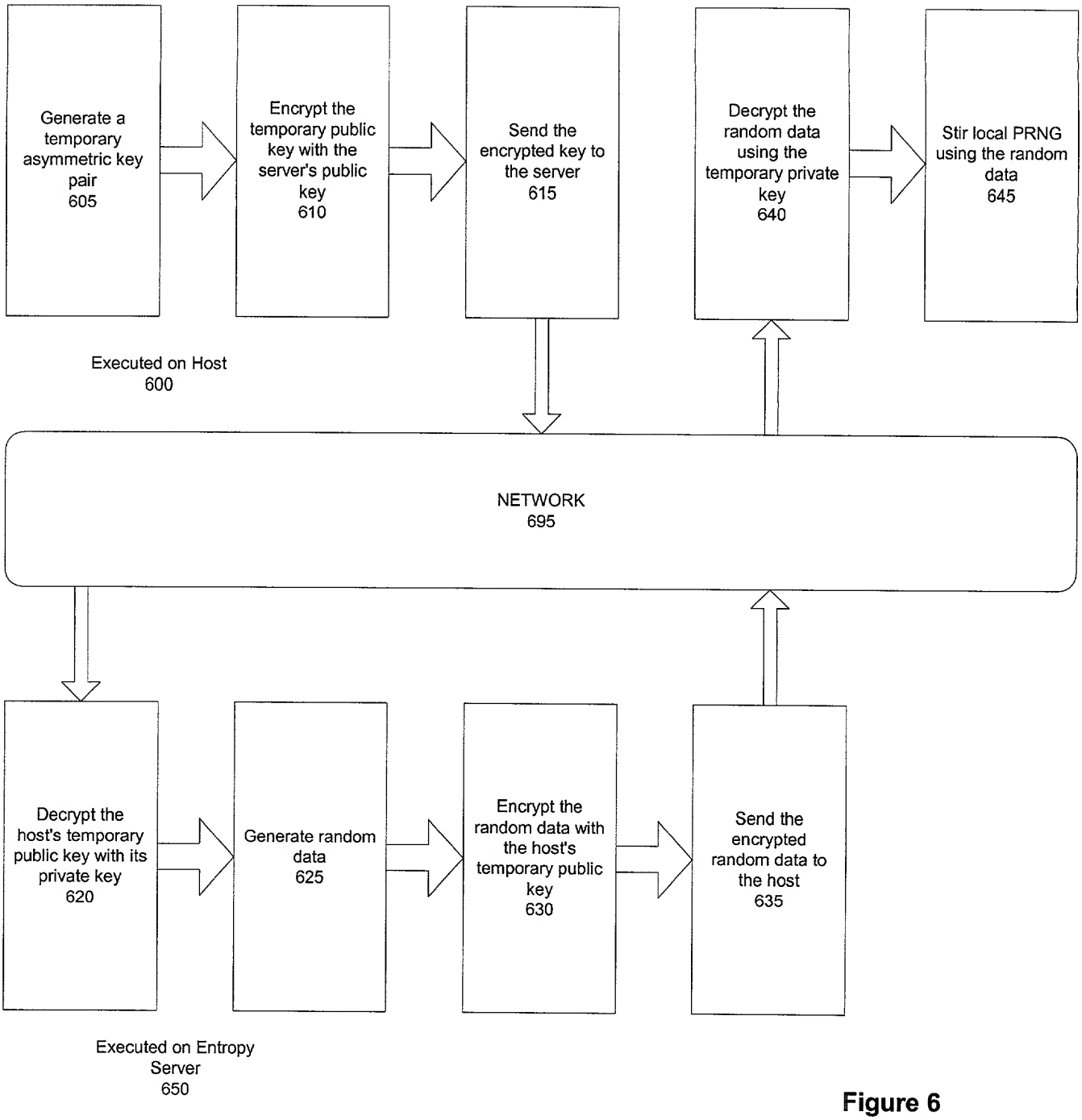
Generate a temporary asymmetric key pair 605
Encrypt the temporary public key with the server's public key 610
Send the encrypted key to the server 615
Decrypt the random data using the temporary private key 640
Stir local PRNG using the random data 645
Executed on Host 600
NETWORK 695
Decrypt the host's temporary public key with its private key 620
Generate random data 625
Encrypt the random data with the host's temporary public key 630
Send the encrypted random data to the host 635
Executed on Entropy Server 650

Figure 6

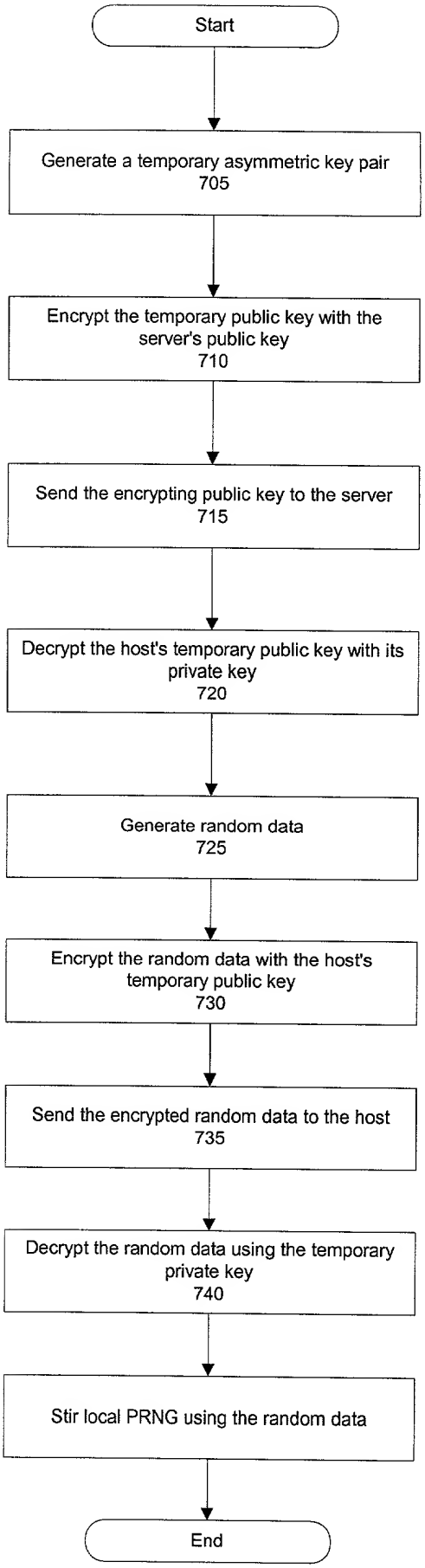
Start
Generate a temporary asymmetric key pair
705
Encrypt the temporary public key with the server's public key
710
Send the encrypting public key to the server
715
Decrypt the host's temporary public key with its private key
720
Generate random data
725
Encrypt the random data with the host's temporary public key
730
Send the encrypted random data to the host
735
Decrypt the random data using the temporary private key
740
Stir local PRNG using the random data
End

Figure 7